State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

December 09, 2014

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2014-089

DATE(S) ISSUED:

12/09/2014

SUBJECT:

Multiple Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS14-083)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Excel that could result in remote code execution. Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Two vulnerabilities have been identified in Microsoft Excel that could allow remote code execution. These vulnerabilities are caused due to the way that Microsoft Excel handles specially crafted Excel files.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS14-083

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6360

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6361